

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Internet op het werk - privé-leven en e-mail = Web au travail - vie privée et courrier électronique

Poullet, Yves

Publication date:
2002

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 2002, *Internet op het werk - privé-leven en e-mail = Web au travail - vie privée et courrier électronique..*

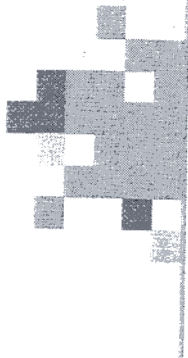
General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



Conférence du C.I.R.B. C.I.B.G.-conferentie

Internet op het werk – privé-leven en e-mail

Web au travail – Vie privée et courrier électronique

4/10/2002

Centre Diamant Centrum

Programme

Matinée

9h00 : **Hervé Feuillien et Robert Herzeele**, Directeur Général et Directeur Général adjoint du C.I.R.B., *Mot de bienvenue.*

9h10 : **Guy Vanhengel**, Ministre du Gouvernement bruxellois, *Introduction sur le sujet*

9h25 : **Rosette Vandenbroucke**, ICT Manager IIHE, Partenaire du groupe de recherche en télématique HELIOS, *Introduction et réflexion sur base de l'historique de l'Internet.*

9h35 : **Yves Poulet**, Directeur du CRID (Centre de Recherche Informatique et Droit), *Protection de la vie privée des citoyens, traitement de l'information par l'administration électronique, reconnaissance juridique de la signature électronique.*

9h50 : **Carine Doutrelepon**, Professeur à l'ULB, Avocate, *La propriété intellectuelle sur le web.*

10h05 : **Anne-Marie Appelmans**, Secrétaire Générale FGTB-Bruxelles, *Convention collective et point de vue du syndicat par rapport au contrat d'emploi et à l'utilisation du web au travail.*

10h20 : **Paul De Hert**, Docent aan de VUB- Hoofddocent aan Leiden, *Considérations critiques sur le cadre légal belge et place de la convention collective. Les techniques de surveillance d'utilisation du web et du mail par les employés.*

10h35 : Pause

11h00 : Débat animé par **Alain Jenotte**, Journaliste, Le Soir, et par **Peter Arijs**, ICT Manager aan het Ministerie van het Brussels Hoofdstedelijk Gewest (MBHG).

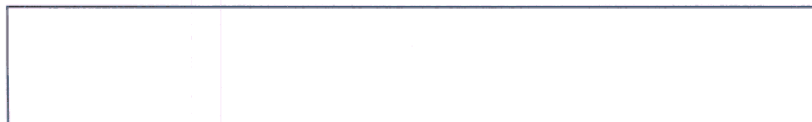
Le lunch de midi sera un moment d'échanges, suite à l'intervention de Monsieur le **Baron Georges Jacobs**, Président de l'UCB, basée sur « *La convention européenne - l'enjeu technologique* ».

L'après-midi, à 14 h, hébergera divers stands de **démonstration de projets et d'applications** informatiques installées chez nos différents partenaires.

15h30- 16h30 : thème et débat

Catherine Parmentier, Chief Executive Officer de Eurocities (dont TeleCities fait partie), *Objectifs e-Europe 2005.*

Hervé Feuillien et Robert Herzeele, Directeurs généraux du C.I.R.B., *Bilan de l'E-Gov et des E-Communes à Bruxelles, Objectifs.*



Programma

Morgen

9 uur : **Hervé Feuillien** en **Robert Herzele**, Directeur generaal en Adjunct-directeurgeneraal van het CIBG, *Welkom word.*

9 uur 10 : **Guy Vanhengel**, Minister van de Brusselse Hoofdstedelijke regering, *Inleiding over het onderwerp.*

9 uur 25: **Rosette Vandenbroucke**, ICT Manager IIHE, Lid van het Telematica-onderzoeksteam HELIOS, *Inleiding en overdenking op basis van de historie van het Internet.*

9 uur 35: **Yves Poulet**, Directeur van het CRID (Centre de Recherche Informatique et Droit), *Bescherming van de persoonlijke levenssfeer van de burgers, informatieverwerking via elektronische administratie, juridische erkenning van de elektronische handtekening.*

9 uur 50: **Carine Doutrelepon**, Professor aan de ULB, Advocate, *De intellectuele eigendom op het Internet.*

10 uur 05 : **Anne-Marie Appelmans**, Secretaris-Generaal van het ABVV-Brussel. *Collectieve overeenkomst en syndicaal standpunt tegenover de arbeidsovereenkomst en het gebruik van het Internet op het werk.*

10 uur 20 : **Paul De Hert**, Docent aan de VUB - Hoofddocent in Leiden, *Kritische beschouwingen over het Belgische wettelijke kader en plaats van de collectieve overeenkomst. Bewakingstechnieken voor het gebruik van het Internet en e-mail door werknemers.*

10 uur 35 : Pauze

11 uur: **Debat** onder de leiding van **Alain Jenotte**, journaliste bij Le Soir, en **Peter Arijs**, ICT Manager aan het Ministerie van het Brussels Hoofdstedelijk Gewest (MBHG).

Tijdens de lunch zal van gedachten gewisseld kunnen worden over de lezing door **Baron Georges Jacobs**, Voorzitter van UCB, die het zal hebben over «*De Europese Conventie en de technologische uitdaging* ».

Na de middag tenslotte, om 14 uur, zal de aandacht gaan naar allerlei **stands waar wij informaticaprojecten en -toepassingen zullen demonstreren**, die bij onze diverse partners geïnstalleerd werden.

15 uur 30- 16 uur 30: thema en debat

Catherine Parmentier, Chief Executive Officer van Eurocities (waarvan TeleCities deel uitmaakt), *Doelstellingen e-Europe 2005.*

Hervé Feuillien en Robert Herzele, Directeurs generaal van het CIBG, *Balans van E-Gov en E-Gemeenten in Brussel. Doelstellingen.*

--	--	--

Yves POULLET

Protection de la vie privée des citoyens, traitement de l'information par l'administration électronique, reconnaissance juridique de la signature électronique.

Curriculum vitae : Licencié en philosophie, Docteur en droit, Yves Poulet est aujourd'hui Directeur du CRID, Doyen de la faculté de droit des FUNDP, membre de la Commission belge de Protection de la vie privée, auteur de nombreux ouvrages dont un 'Guide pour la diffusion de l'information publique : comment améliorer la diffusion de l'information publique et faciliter l'accès du citoyen aux données publiques ?', Yves Poulet, Dominique Dieng, Séverine Dusollier.

Pour une cyberadministration "citoyenne" : Propos pertinents et impertinents.

1. Au moment où **l'Administration vit une révolution « copernicienne »**, notre propos est d'en souligner l'enjeu pour la citoyenneté et d'éviter certaines dérives.

Les promoteurs de la cyberadministration agitent à plaisir les avantages que les citoyens pourraient tirer d'une administration plus accessible, et aux services plus efficaces.

Chaque individu doté d'une carte et d'une signature électronique pourra grâce à ce « sésame » ouvrir à partir de guichets dits uniques les portes des différentes administrations et obtenir rapidement les documents souhaités. Finies les queues qui souvent aboutissent devant un fonctionnaire pas toujours agréable à un « il vous manque un document », « votre demande sera traitée en temps utile » ou, pire, « revenez plus tard ». Les vertus d'Internet et des réseaux « Intranet » qui seront demain déployés entre nos administrations augurent d'un service meilleur. La requête initiée et signée par le citoyen depuis l'écran de son ordinateur permettra à l'Administration d'obtenir elle-même des autres administrations, qu'elles soient fédérales, régionales, communautaires, communales demain européennes, l'ensemble des documents nécessaires et, système d'aide à la décision aidant, la réponse à la requête. La généralisation de l'utilisation d'un identifiant unique permettra cette efficacité nouvelle. Le précédent de la Banque Carrefour sert de modèle à ces développements.

Nul doute qu'une telle construction déjà planifiée par le responsable du plan Copernic répond à la demande de nombre de citoyens. Il serait bien fou celui qui s'y opposerait au nom d'un conservatisme de mauvais aloi.

2. Cependant, une telle construction suscite des craintes diffuses : on évoque le « **Big Brother** » que pourrait constituer une Administration dorénavant totalement intégrée. Il faut bien reconnaître que les documents qui servent de base aux discussions gouvernementales actuelles n'ont rien de rassurant. Le modèle proposé suit la logique certes respectable d'une amélioration de l'efficacité et de la rentabilité administrative. L'idée d'un numéro unique lisible sur la carte d'identité devenue numérique commun à l'ensemble des administrations autorise l'ensemble des interconnexions possibles entre elles. Certes, le document insiste sur la nécessité d'une sécurité des interconnexions, de la proportionnalité de celles-ci aux besoins légitimes des administrations mais qui jugera de cette proportionnalité, si ce n'est des comités tellement proches des administrations qu'on peut craindre que les décisions y prises suivent plus la logique des citoyens. Le précédent du Comité de surveillance de la banque Carrefour en témoigne.

En outre, une fois les réseaux mis en place et leurs larges potentialités découvertes ; on peut craindre que l'utilisation de ceux-ci soit toujours plus réclamée. Ainsi, l'existence de diverses banques de données au sein de la sécurité sociale justifie-t-elle dès aujourd'hui leur croisement pour espérer un contrôle bien plus efficient des assurés sociaux et de leurs employeurs.

--	--

On rappellera l'ancienne proposition du Ministre des Finances, de développer un vaste réseau permettant de collecter auprès des administrations fiscales, sociales, les organisations caritatives, etc. toutes les informations nécessaires afin d'établir pour chaque citoyen un projet de déclaration fiscale que celui-ci n'aurait plus qu'à signer.

3. Quatre dossiers récents étudiés par la Commission de protection de la vie privée illustrent ces craintes : le premier a eu les honneurs de la presse. Il s'agit du recensement de l'INS. Ce qui était en cause, ce n'était pas tant l'indiscrétion des questions contenues dans le formulaire papier remis à chaque ménage mais à la limite les interconnexions que l'INS s'apprêtait à opérer sur base du numéro de registre national pour interroger d'autres banques de données administratives, système de collecte de données qui lui permettra dorénavant et avantageusement de se passer de toute collecte auprès des citoyens. Le deuxième dossier est la réforme du registre national introduite par le gouvernement visant notamment à libéraliser l'utilisation du numéro de registre national et à introduire la carte d'identité électronique. Le troisième est la création projetée d'une banque-carrefour des entreprises qui, dans un souci de simplification administrative, permettra à chaque administration de connaître les données minimales d'une entreprise, notion entendue au sens le plus large (y compris un avocat ou un médecin), la localisation des données administratives de celle ci et dès lors l'interrogation automatique de ces banques de données sans devoir désormais en référer à l'entreprise. Enfin, un quatrième dossier peut être évoqué : il s'agit de la création d'un centre fédéral d'expertise de la santé qui pourra coupler au service d'un meilleur contrôle des acteurs de la santé et d'une aide à la définition d'une politique de la santé, les données de la sécurité sociale et de la santé.

4. Faut-il rejeter ce modèle de développement de la cyberadministration ? Un autre modèle pourrait lui être préféré : celui dit du « self service » où les technologies auraient pour seul but la simplification administrative au bénéfice du citoyen. Ainsi, dans l'exemple fiscal repris ci-dessus, on peut imaginer que ce soit lui-même qui puisse initier la collecte des informations auprès des diverses administrations et ce à partir de son ordinateur et proposer, via le réseau, à l'Administration fiscale le produit de sa collecte ainsi facilitée par l'utilisation des technologies nouvelles.

Sans doute, objectera-t-on à ce second modèle qu'il favorise certaines couches de la population, plus initiées aux arcanes des réseaux modernes d'information. A cet égard, le premier modèle est, nous dira-t-on, plus égalitaire et plus efficace.

Ce premier modèle, s'il est acceptable, devrait cependant mieux prendre en compte

- les libertés du citoyen et l'impact qu'un projet aussi bureaucratique et déresponsabilisant pourrait avoir sur l'opinion publique ;
- la dimension « multiniveaux »(fédéral, régional, communautaire, communal) du dossier ;
- l'impact sur l'administration elle-même (la perte d'emploi, la requalification du personnel, etc.) ;
- les dangers d'une dérive du système en cas d'arrivée d'un pouvoir totalitaire.

5. Ainsi, il nous semble, afin de nous protéger

- qu'un débat démocratique devrait avoir lieu comme déjà demandé par la Commission de protection de la vie privée lors du débat sur l'introduction de la carte SIS ;
- que ce débat doit être piloté par le Parlement lui-même sur proposition du gouvernement et après avoir entendu tous les acteurs intéressés (groupement de défense des citoyens, C.P.V.P....).
- que certains droits doivent être consacrés pour le citoyen : droit de conserver une procédure « papier » ; droit de ne pas se voir appliquer des mesures non demandées sur base d'une décision fondée sur l'utilisation des I.C.T., droit à une totale transparence des flux générés par un dossier (Cf. infra, n° 6) ;

--	--

7. **Si les lois** vie privée permettent une cyberadministration plus transparente et plus soucieuse du respect des libertés du citoyen elles ne sont point les seules : les lois d'accès ou de publicité de l'administration (chez nous la loi du 10 juillet 1994 relative à la publicité de l'administration) constituent à cet égard un complément utile et surtout élargissent le propos. Nombre de pays étrangers, les Etats-Unis (cf. l'Electronic Freedom of Information Act de 1996) les premiers mais depuis le Royaume-Uni, la Suède, etc. ont modernisé leur loi sur l'accès à l'information en affirmant le principe du droit à un accès électronique aux dossiers de l'Administration, instituant le devoir de cette dernière d'utiliser les technologies nouvelles pour rendre accessibles les données sur lesquelles l'Administration fonde sa décision ou son action.

En poussant plus loin le raisonnement, n'existe-t-il pas pour l'individu, un droit à ce que les canadiens ont appelé un « temps d'ordinateur » c'est-à-dire un droit à une programmation qui permette à l'Administration non seulement de répondre directement à un droit d'accès mais également d'expliquer le raisonnement suivi lors d'une décision, les sources de l'information utilisée, les modes de contestation, voire la possibilité d'une saisine en ligne d'une « juridiction » administrative.

8. Au-delà de cette consécration d'un **devoir de l'administration de répondre aux demandes** des citoyens, se voit de plus en plus consacrée par des versions plus modernes de ces lois dites d'accès aux documents administratifs, une obligation positive de l'Etat de mettre à disposition des citoyens et ce de manière électronique un certain nombre d'informations sur ses activités ou le résultat de ses activités . L'administration qui dans le cadre de ses compétences collecte et traite de l'information sur l'environnement, les entreprises, les ménages se voit contrainte de les diffuser. Cette obligation croît dans la mesure où ces collectes et s se voient facilités par les moyens technologiques modernes et que ces mêmes moyens permettent (que l'on songe à Internet ou aux CD rom) de diffuser facilement et à des coûts marginaux l'information en résultant.

Prenons quelques exemples : l'Etat collectera demain grâce à la banque-carrefour des entreprises des informations permettant de recenser les entreprises d'un secteur d'activité, leur localisation et l'importance de leur production.

D'autres banques de données fourniront des données sur leur environnement (la fréquentation des voies d'accès (Office de la circulation routière), l'habitat (cadastre), le prix moyen du produit fabriqué par cette entreprise dans le marché commun ou en Belgique (le service des prix), etc.). Toutes ces informations peuvent être utiles pour une entreprise déjà installée ou cherchant à s'implanter. Un citoyen de même souhaitera pouvoir consulter aisément l'agenda du conseil communal, la liste des crèches de sa ville, les divers travaux de voirie qui peuvent entraver la circulation, la liste des permis de bâtir octroyés, etc. .

Diverses circulaires françaises ont donné un sens à ce « droit du citoyen à l'information essentielle » que Jospin appelait de ses vœux, lors de son discours célèbre d'Hourdin de 1999. Que ce soit en matière de réglementation, d'environnement, de santé ou de sécurité, il est urgent que chaque Administration concernée en concertation avec les représentants des citoyens, définisse ce qu'elle entend dans son secteur par cette information nécessaire pour qu'un citoyen puisse exercer librement ces choix d'existence et utilise les technologies modernes de communication pour la diffuser.

9. Et **la carte d'identité électronique** voire la signature électronique dans tout cela ? Elles apparaissent comme les corollaires souhaitables d'un dialogue électronique entre le citoyen et l'administration. Ceci dit, à propos de la carte, premièrement, on peut souhaiter minimiser le nombre d'informations lisibles sur la carte. En particulier, faut-il nécessairement que le numéro de registre national y figure alors même que pour les personnes autorisées à le consulter, on peut prévoir un accès électronique en lecture.

La digitalisation de la photo du porteur de la carte autorise la copie aisée sur d'autres supports de cette photo. Par ailleurs, faut-il autoriser que cette carte puisse devenir porteuse de dossiers, qu'il s'agisse du dossier médical d'urgence, du dossier « habilitation sécurité sociale » (s'il y avait confusion de la carte SIS et de la carte d'identité), etc. ? La question de la gestion de ces dossiers et



de leur accès soulève des difficultés nombreuses, en cas de perte de la carte et multiplieraient les obligations de présentation de la carte d'identité, ce qui n'est point souhaitable et contraire aux législations actuelles limitant fortement les personnes autorisées à exiger la carte.

En toute hypothèse, il importe que la présentation de la carte d'identité et l'utilisation de la signature électronique ne puissent être exigées que lorsque les nécessités du service administratif les requièrent.

10. La signature électronique qui pourrait être supportée par la carte permet des transactions électroniques, garantit la valeur juridique des documents ainsi signés mais également, utilisée par le fonctionnaire dans le cadre de la cyberadministration, permet des vérifications automatiques ou a posteriori de la légitimité des accès à certaines informations. A propos de ce dernier point, on ne peut qu'appuyer l'idée d'un registre des certificats des signatures des fonctionnaires mentionnant leur qualité et compétence et autorisant ainsi tant les contrôles d'accès que l'identification du signataire et des ses compétences.

A propos de la signature électronique officielle des citoyens, il n'est pas évident que la nature des transactions passées avec l'administration constitue à elle seule aux yeux des autorités européennes une justification des procédures particulières requises pour sa création.

Ne peut-on à cet égard se contenter des signatures avancées offertes sur le marché ? Certes, la signature électronique liée à la carte d'identité dispose de par la procédure officielle de vérification de l'identité de la personne demanderesse d'une forte valeur mais cette signature électronique « officielle » sert-elle uniquement dans les relations entre le citoyen et l'administration ou peut-elle également servir dans les relations entre une entreprise et son client ?

Si cette dernière hypothèse est retenue et on peut supposer que le secteur privé fera une forte pression pour que ce soit le cas vu la quasi gratuité de la délivrance des certificats et la haute valeur des certificats émis, il est facilement imaginable que des entreprises privées souhaiteront coupler leur carte à microprocesseur à l'utilisation de la carte d'identité voire intégrer leur microprocesseur à la carte d'identité, afin de pouvoir vérifier la signature de la personne souhaitant l'accès à leurs services.

Cette réflexion soulève la crainte d'une généralisation de la présentation de la carte d'identité pour l'obtention de services privés et la possibilité pour les prestataires de ces services de pouvoir accéder en lecture à l'ensemble des informations lisibles électroniquement et présentes sur la carte. Ce risque est aggravé si la carte d'identité dans le futur devient le support de dossiers électroniques.

11. Une seconde réflexion s'inquiète de la manière dont certaines administrations pourraient favoriser l'utilisation des signatures électroniques en accordant des priorités ou avantages à ceux qui recourent à des procédures d'authentification électronique et aux procédures on line.

Il est important qu'aucune discrimination ne soit directement ou indirectement introduite vis à vis des personnes qui souhaiteraient conserver une procédure papier et les modes traditionnels d'authentification.

12. Voilà la « cyberadministration » que nous appelons de nos vœux citoyens. C'est à certaines conditions – et c'est le rôle d'un débat démocratique de les définir – qu'elle n'apparaîtra pas réductrice de nos libertés mais conjuguera une efficacité meilleure de nos administration avec la promotion de ces libertés.

Y. Pouillet

Doyen de la faculté de droit des FUNDP

Directeur du Crid

y.pouillet@fundp.ac.be

<http://www.crid.ac.be>

--	--

Bescherming van de persoonlijke levenssfeer van de burgers, informatieverwerking via elektronische administratie, juridische erkenning van de elektronische handtekening.

Curriculum vitae : Licentiaat in de Wijsbegeerte, Doctor in de Rechten, vandaag is Yves Poulet Directeur aan het CRID, Deken van de Rechtsfaculteit van de FUNDP, lid van de Belgische commissie voor de bescherming van de persoonlijke levenssfeer, Professor aan het FUNDP, auteur van talrijke werken waarvan een " Gids voor de verspreiding van openbare informatie: hoe de openbare informatie verspreiden en hoe de toegang tot openbare gegevens voor de burger te vergemakkelijken? ", Yves Poulet, Dominique Dieng, Séverine Dusollier.

Naar een maatschappelijk verantwoorde cyberadministratie: een denkoefening.

1. Net nu de Administratie een ware omwenteling meemaakt, willen wij graag toelichten wat hiervan de inzet is voor de burger en mogelijke misbruiken aan de kaak stellen.

De voorstanders van de cyberadministratie schuiven maar al te graag de voordelen naar voor, die de burgers zouden kunnen halen uit een beter toegankelijke administratie en efficiënter werkende diensten.

Iedereen die een elektronische identiteitskaart en handtekening op zak heeft – virtueel dan – krijgt als bij toverslag toegang tot de zogenaamde unieke loketten en meteen tot de verschillende administraties, en komt heel snel bij de gevraagde documenten. Weg met de eindeloze wachtrijen met aan het einde een niet-altijd-even-vriendelijke ambtenaar die iets spuit in de zin van «u heeft nog een extra document nodig», «uw aanvraag zal te gepasten tijde behandeld worden» of erger nog, «komt u later maar eens terug». Het Internet en de intranetten die straks onze administraties zullen bevolken, stellen een betere dienstverlening in het vooruitzicht. Op zijn PC dient de burger zijn aanvraag in, ondertekent die en stuurt ze door. Vanaf dan kan de administratie in kwestie bij andere administraties – federaal, gewestelijk, communautair en straks ook Europees – alle nodige documenten opvragen, en mits de nodige besluitondersteunende systemen, ook het antwoord op de vraag. Een veralgemeend gebruik van een unieke identifier moet de weg effenen naar vernieuwde efficiëntie. De Kruispuntbank kan hier model staan voor deze ontwikkelingen.

Het lijkt geen twijfel dat een dergelijke constructie, die al door de verantwoordelijke van het Copernicusplan ingecalculeerd was, tegemoetkomt aan de vraag van heel wat burgers. Wie zich hiertegen vanuit een misplaatst conservatisme zou verzetten, is niet goed bezig.

2. Wat niet belet dat deze ontwikkeling nogal wat diffuse angsten oproept: de angst voor een voortaan volledig geïntegreerde Administratie, die tot een soort «**Big Brother**» uitgroeit. En toegegeven, de documenten die momenteel als grondslag dienen voor de besprekingen op regeringsvlak, hebben niets geruststellends. Het voorgestelde model houdt zich aan de lovenswaardige logica die een efficiënter en rendabeler overheidsapparaat wil zien ontstaan. Het idee van één enkel elektronisch nummer op de identiteitskaart dat gemeenschappelijk is voor alle administraties, effent meteen de weg naar interconnecties tussen die administraties.

Het document beklemtoont evenwel de noodzaak van beveiliging van deze interconnecties, wijst op het feit dat deze in verhouding moeten staan tot de rechtmatige behoeften van de administraties. Maar wie zal erover oordelen of dat zo is, tenzij een handvol comités die zo dicht bij de administraties zelf staan, dat de beslissingen die er uiteindelijk genomen worden, de logica van de burgers niet volgen. Wat gebeurd is met het Toezichtscomité van de Kruispuntbank bewijst dit. Bovendien valt te vrezen dat, eens de netwerken goed en wel geïnstalleerd en hun enorme mogelijkheden ten volle doorgedrongen zijn, het gebruik ervan steeds intensiever zal worden.

--

Zo vormt het bestaan van de diverse databanken binnen de sociale zekerheid vandaag de dag de verantwoording om ze met elkaar te kruisen en hopelijk te komen tot een veel efficiëntere controle van de sociaal verzekerden en hun werkgevers. Wij verwijzen ook naar het oude voorstel van de Minister van Financiën voor het uitbouwen van een grootschalig netwerk om bij de fiscale en sociale administratie, de liefdadigheidsinstellingen, enz. alle informatie in te zamelen die nodig is om voor elke burger een ontwerp van belastingaangifte op te stellen, die de burger dan alleen nog hoeft te ondertekenen.

3. Vier recente dossiers die bestudeerd worden door de Commissie voor de bescherming van de persoonlijke levenssfeer, sterken onze vrees: het eerste mocht zich verheugen in de nodige weerklink in de pers. Wij hebben het over de volkstelling van het NIS. Wat in vraag gesteld werd, was niet zozeer de indiscretie van de vragen die gesteld werden op het document dat elk gezin in de bus kreeg, maar wel de interconnecties die het NIS van plan was uit te voeren op basis van het rijksregisternummer om zo andere administratieve databanken te ondervragen. Dankzij een dergelijk gegevensinzamelingssysteem zou het NIS voortaan de burger niet eens meer nodig hebben.

Het tweede dossier betreft de door de regering voorgestelde hervorming van het rijksregister, die het gebruik van het rijksregisternummer moet liberaliseren en uiteindelijk moet leiden tot de invoering van de elektronische identiteitskaart. Het derde is de geplande oprichting van een kruispuntbank van ondernemingen: met het oog op administratieve vereenvoudiging zouden alle administraties hierdoor toegang krijgen tot de minimale gegevens betreffende een onderneming – in de ruime zin van het woord, inclusief advocaten of artsen) – zouden zij weten waar deze administratieve gegevens zich bevinden en deze databanken automatisch kunnen ondervragen zonder daarvoor bij de onderneming te gaan aankloppen. Tot slot nog een vierde dossier in dit verband: de oprichting van een federaal kenniscentrum voor de gezondheidssector, dat de gegevens van de sociale zekerheid en gezondheid zal koppelen aan een betere controle van de spelers in de gezondheidssector en de uittekening van een gezondheidsbeleid.

4. Moeten wij dit model van de cyberadministratie dan verwerpen? Misschien moet een ander model de voorkeur krijgen: het zogenaamde «self service» model, waarbij de technologieën alleen moeten leiden tot administratieve vereenvoudiging ten dienste van de burger. In ons voorbeeld van de belastingaangifte van daarnet, kunnen wij ons voorstellen dat het de burger zelf is die vanaf zijn PC informatie gaat verzamelen bij de diverse administraties, en de Belastingadministratie dan, alweer via het Internet, de vrucht van zijn inzamelingswerk voorlegt.

Tegen dit tweede model zal als bezwaar allicht aangevoerd worden dat het bepaalde lagen van de bevolking die beter vertrouwd zijn met moderne informatienetwerken, bevoordeelt. Op dat punt is het eerste model, zo zal het luiden, meer egalitair geschoeid en efficiënter.

Als wij met dit eerste model kunnen leven, moet het wel beter rekening houden met:

- de vrijheden van de burger en de weerslag die een zo bureaucratisch en deresponsabiliserend project kan hebben op de publieke opinie;
- de gelaagdheid van het dossier (federaal, gewestelijk, communautair, gemeentelijk);
- de weerslag op de administratie zelf (jobverlies, herkwalificatie van het personeel, enz.);
- de gevaren i.v.m. misbruik van het systeem indien ooit een totalitair bewind aantreedt.

5. Om ons te beschermen, lijkt ons dan ook

- dat een democratisch debat moet kunnen plaatsvinden, zoals trouwens door de Commissie voor de bescherming van de persoonlijke levenssfeer al gevraagd is naar aanleiding van de invoering van de SIS-kaart;
- dat dit debat geleid moet worden door het Parlement op voorstel van de regering en na het horen van alle betrokken spelers (burgerbelangengroeperingen, CBPL...).
- dat sommige rechten voor de burger behouden moeten blijven: het recht om een «papieren» procedure te volgen; het recht om niet onderworpen te worden aan ongevraagde maatregelen die

--	--

voortvloeien uit een beslissing op basis van ICT; het recht tot volledige transparantie van de stromen die door een dossier veroorzaakt worden (zie verder, nr. 6);

- dat een instantie opgericht moet worden, die echt los staat van de Administratie en die tot taak krijgt een kadaster van de gegevensstromen op te stellen, de wettigheid, het doel en de proportionaliteit van de aanvragen na te gaan. In het ideale geval zou deze instantie de CBPL moeten zijn, die dan handelt onder controle van de federale, gewestelijke of communautaire wetgeving;

- dat technische maatregelen genomen worden waardoor de controle op de naleving van deze principes, automatisch georganiseerd wordt. In dit verband moet strenge regelgeving uitgewerkt worden in verband met de verplichting voor ambtenaren om hun toegangsaanvragen te ondertekenen, het bewaren van sporen betreffende de opvragingen van gegevens en vooral de opstart van geautomatiseerde controlesystemen die ongeoorloofde aanvragen moeten voorkomen;

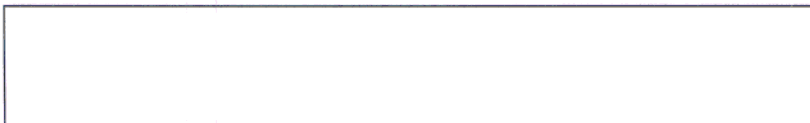
- dat het beginsel van de functionele scheiding tussen de administraties – van oudsher de beste waarborg i.v.m. de bescherming de burger – bevestiging krijgt, ook al moeten uitzonderingen mogelijk zijn en worden die allicht steeds talrijker. Zou men daarom niet opnieuw moeten nadenken over verschillende identificatienummers per administratieve sector, zoals in sommige landen en recent ook nog in België gesuggereerd werd: zo bijvoorbeeld een gezondheidsnummer, een gerechtelijk nummer, allebei losstaand van het rijksregisternummer, van het nummer van de sociale zekerheid. Dergelijk gebruik van onderscheiden nummers in gevoelige sectoren zou een betere controle op de interconnecties tussen sectoren mogelijk maken, want in dat geval zouden voor die interconnecties conversietabellen vereist zijn, waarvan het gebruik gereguleerd en beveiligd kan worden.

- tot slot dat elke administratieve sector moet kunnen terugvallen op een «gedetacheerde voor gegevensbescherming» die tot taak krijgt om, volgens het model dat voorgesteld wordt door de Europese richtlijn inzake gegevensbescherming, in volledige onafhankelijkheid toe te zien op de naleving van de beginselen van de wetgeving op de persoonlijke levenssfeer, op de opleiding van de ambtenaren m.b.t. deze beginselen, op de beveiliging van netwerken en bestanden (betrouwbaarheid en vertrouwelijkheid van de gegevens, enz.).

6. Ons voorstel houdt daar niet op. Het bezit van informatie, zo wordt gezegd, werkt machtsversterkend, en het lijkt geen twijfel dat dit het geval is in de relatie tussen een steeds transparantere burger en een steeds almachtiger cyberadministratie. Dit gegeven brengt ons bij de eis dat de inzet van technologieën ook de macht van de burger in zijn relatie met de overheid zou versterken, en dit in dezelfde mate als de macht van die administratie door de inzet van technologieën versterkt wordt. Wij hebben hier te maken met het proportionaliteitsbeginsel: daarbij geldt dat het evenwicht tussen de belangen van de burger en die van de administratie – zoals het van oudsher opgevat en verzekerd werd, met name door een opdeling van de administraties – niet ten gronde verstoord mag worden door de technologische ontwikkeling en het ongecontroleerde gebruik van technologieën.

Dit streven naar een hersteld evenwicht in de relatie burger – administratie, vindt in het gebruik van technologieën een oplossing, dit keer ten dienste van de burger. Zo veronderstelt het recht op informatie, zoals dat bevestigd werd door de wetten betreffende de bescherming van gegevens, volgens ons dat de burger die voor een elektronisch loket staat, niet alleen duidelijk moet weten welk gebruik gemaakt zal worden van de gegevens die hij overmaakt, maar ook welke gegevens via de e-administratie bij andere administraties opgevraagd kunnen worden om zijn dossier te vervolledigen.

Dat toegangsrecht zou een elektronisch toegangsrecht moeten worden, waardoor het voor de burger mogelijk wordt om zijn dossier elektronisch op te volgen, om te weten – via de sporen die bewaard worden van de opvragingen uit de databanken – wie toegang gekregen heeft tot zijn dossier of zijn gegevens. Binnenkort wordt hierover in Zweden een wet gestemd: deze moet zorgen voor meer administratieve transparantie, want hij zal de burger de waarborg geven dat hij zijn dossiers volledig kan volgen, vanaf de opening van het dossier tot en met de archivering ervan. De verplichting die door de wet van 1992 opgelegd werd om toegang te krijgen tot de logica die gevolgd wordt door besluitondersteunende systemen of zogenaamde expertsystemen, zal straks de verplichting opleggen dat de burger kan beschikken over informatie over de werking van deze systemen, of zelfs zelf de werking ervan kan simuleren (systemen voor pensioenberekening, voor belastingheffing of subsidies...).



7. **De wetten op de persoonlijke levenssfeer staan borg voor een transparantere cyberadministratie**, die meer respect heeft voor de vrijheden van de burger. Maar zij doen dat niet alleen: de wetten betreffende de toegang of de openbaarheid van bestuur (bij ons de wet van 10 juli 1994 betreffende de openbaarheid van bestuur) vormen in dat verband een handige aanvulling en verruimen ook de draagwijdte. Heel wat andere landen – de Verenigde Staten (cf. de "Electronic Freedom of Information Act" van 1996) op kop, maar daarna ook Groot-Brittannië, Zweden, enz. – hebben hun wetgeving op de toegang tot informatie gemoderniseerd en het beginsel van het recht op elektronische toegang tot de dossiers van de Administratie bevestigd, waarbij deze laatste de verplichting toekomt nieuwe technologieën te gebruiken om de gegevens waarop de Administratie haar beslissing of handeling baseert, toegankelijk te maken.

En als wij de redenering nog even verder doortrekken, bestaat er voor het individu niet het recht op wat de Canadezen «computer time» noemen, dit wil zeggen het recht op een programmering, waardoor de Administratie niet alleen onmiddellijk op een toegangsrecht kan antwoorden, maar ook uitleg kan verstrekken bij de redenering die bij een beslissing gevolgd wordt, de bronnen van de gebruikte informatie, de manieren om beslissingen te betwisten, zelfs de mogelijkheid voor het on line aanhangig maken van een administratieve «uitspraak»?

8. Naast deze bevestiging van de plicht voor de overheid om op **vragen van de burgers** te antwoorden, komt er – door modernere versies van de wetten op de toegang tot administratieve documenten – een positieve verplichting voor de Staat om bepaalde informatie over zijn activiteiten of het resultaat van deze activiteiten, ter beschikking te stellen van de burger en dit via elektronische weg. De administratie, die vanuit haar opdracht informatie inzamelt en verwerkt over milieu, ondernemingen, gezinnen, enz., wordt verplicht deze informatie te verspreiden. Die verplichting zal grotere vormen aannemen naarmate die gegevensinzameling door de inzet van moderne technologische middelen makkelijker wordt, en diezelfde middelen – denken wij daarbij aan het Internet en CD-ROM – ervoor zorgen dat die informatie makkelijk en tegen marginale kosten verspreid kan worden.

Enkele voorbeelden: straks gaat de Staat via de kruispuntbank ondernemingen informatie verzamelen waardoor het mogelijk wordt een bestand samen te stellen met de ondernemingen van een bepaalde sector, plus informatie over waar zij gevestigd zijn en hoe groot hun productie is. Andere databanken zullen gegevens verstrekken over hun omgeving (gebruik van de toegangswegen, Dienst voor het Wegverkeer), hun gebouwen (kadaster), de gemiddelde prijs van het product dat deze onderneming vervaardigt op de gemeenschappelijke markt of in België (Dienst Prijzen), enz. Al deze gegevens kunnen nuttig zijn voor een onderneming die al geïnstalleerd is of een vestiging wil starten.

Ook de burger zal makkelijk de agenda voor de volgende gemeenteraad willen raadplegen, of een lijst met kinderdagverblijven in zijn gemeente, de verschillende wegenwerken die het verkeer kunnen hinderen, de lijst met goedgekeurde bouwvergunningen, enz. Diverse Franse omzendbrieven hebben invulling gegeven aan dit «recht van de burger op essentiële informatie», waarachter Jospin zich voluit schaarde in zijn beroemde toespraak van Hourdin in 1999. Zowel op het vlak van regelgeving, milieu, gezondheid of veiligheid is het dringend noodzakelijk dat elke betrokken Administratie, in overleg met de vertegenwoordigers van de burgers, bepaalt wat zij bedoelt met deze noodzakelijke informatie, opdat de burger deze bestaanskeuzes vrij zou kunnen uitoefenen en de moderne communicatietechnologieën zou gebruiken om ze te verspreiden.

9. En wat met **de elektronische identiteitskaart** of zelfs de elektronische handtekening in dit alles? Zij lijken de wenselijke randverschijnselen in de elektronische dialoog tussen burger en administratie. Eerst dit in verband met de kaart: het aantal gegevens dat op de kaart af te lezen valt, moet tot een minimum beperkt worden. Is het bijvoorbeeld noodzakelijk dat het rijksregisternummer erop vermeld staat, als men ervoor kan zorgen dat daartoe bevoegde mensen dat nummer elektronisch kunnen lezen.

De digitalisering van de foto van de kaarthouder maakt het mogelijk dat deze foto makkelijk op andere dragers gekopieerd kan worden. Mag men verder toelaten dat deze kaart ook drager wordt



van allerlei dossiers, bijvoorbeeld het dossier dringende medische hulp, het dossier «sociale zekerheid» (indien er verwarring zou zijn tussen de SIS-kaart en de identiteitskaart), enz.? Het beheer van deze dossiers en de toegang ertoe schept allerlei problemen bij verlies van de kaart en zou het verplichte vertoon van de identiteitskaart frequenter maken, wat geenszins wenselijk is en indruist tegen de huidige wetgeving die het aantal mensen met bevoegdheid om voorlegging van de kaart te eisen, sterk beperkt. Hoe dan ook is het belangrijk dat voorlegging van de identiteitskaart en het gebruik van de elektronische handtekening alleen geëist kunnen worden wanneer de noodwendigheden van de administratieve dienst dit vereisen.

10. **De elektronische handtekening**, die door de kaart ondersteund zou kunnen worden, laat elektronische transacties toe, waarborgt de juridische waarde van elektronisch ondertekende documenten, maar laat de ambtenaar binnen de cyberadministratie ook toe om automatische of a posteriori controles uit te voeren van de wettigheid van bepaalde gegevensopvragingen. In dit verband kunnen wij alleen maar voorstander zijn van het idee van een register met certificaten van de handtekeningen van de ambtenaren, met opgave van hun functie en bevoegdheid, waardoor zowel de toegangscontroles als de identificatie van de ondertekenaar en diens bevoegdheden, mogelijk worden.

In verband met de officiële elektronische handtekening van burgers ligt het niet voor de hand dat de aard van de transacties die met de administraties aangegaan worden, op zich in de ogen van de Europese instanties een verantwoording vormen voor de bijzondere procedures die nodig zijn voor de invoering ervan. Kunnen wij het hier niet stellen met de geavanceerde handtekeningen die reeds op de markt zijn? Zeker is wel dat de elektronische handtekening gekoppeld aan de identiteitskaart, vanwege de officiële procedure tot controle van de identiteit van de aanvrager, een sterke juridische waarde heeft.

Maar dient deze «officiële» elektronische handtekening uitsluitend in de betrekkingen tussen burger en administratie, of kan zij ook dienst doen in de relaties tussen een onderneming en haar klanten? In de veronderstelling van dit laatste – en verwacht mag worden dat de privé-sector druk zal uitoefenen dat dit inderdaad het geval wordt, vanwege de bijna gratis aflevering van de certificaten en de grote waarde van de uitgegeven certificaten – is het makkelijk denkbaar dat privé-ondernemingen hun chipkaart willen koppelen aan het gebruik van de identiteitskaart, of die chipkaart zelfs in de identiteitskaart willen integreren om zo de handtekening te kunnen checken van een persoon die toegang wenst tot haar diensten. Door dit alles groeit de vrees dat mensen om de haverklap hun identiteitskaart zullen moeten voorleggen, ook om privé-diensten te bestellen, waarbij de verstrekkers van deze diensten de mogelijkheid krijgen om ook alle andere, elektronisch leesbare informatie op de kaart, in te kijken. Dit risico wordt nog groter indien de identiteitskaart in de toekomst ook elektronische dossiers zal bevatten.

11. Voorts kunnen vragen rijzen over **de manier waarop sommige administraties het gebruik van elektronische handtekeningen** zullen willen bevorderen door voorrang of voordelen toe te kennen aan wie gebruik maakt van elektronische authenticatieprocedures en on line procedures.

Belangrijk is dat geen enkele discriminatie – noch rechtstreeks noch onrechtstreeks – ontstaat tegenover mensen die vasthouden aan een procedure op papier en aan traditionele authenticatiemethodes.

12. Tot zover **de «cyberadministratie»** die wij als burgers graag willen zien ontstaan. Mits aan bepaalde voorwaarden voldaan is – voorwaarden die een democratisch debat moet vastleggen – zal deze cyberadministratie onze vrijheden niet inperken maar zal zij integendeel een efficiënter functionerende administratie verzoenen met een uitbreiding van die vrijheden.

Y. Pouillet

Deken van de Rechtsfaculteit van de FUNDP

Directeur van het Crid

y.pouillet@fundp.ac.be

<http://www.crid.ac.be>

